CLAIMS

We claim:

1. A method of operating a cryptographic data processing system that comprises a host processor, a system memory coupled to the host processor, and a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory, the method comprising:

loading at least one operand from the system memory to the local memory; and

executing an instruction using the cryptographic processor that references the at least one operand using a first relative position in the local memory.

2. The method of Claim 1, wherein loading at least one operand from the system memory to the local memory comprises loading at least two operands from the system memory to the local memory, and executing the instruction comprises:

executing the instruction using the cryptographic processor that references a first one of the operands using the first relative position in the local memory and a second one of the operands using a second relative position in the local memory, the first and second relative positions being contiguous with one another.

3. The method of Claim 2, wherein the first one of the operands and the second one of the operands comprise different numbers of bits.

4. The method of Claim 1, wherein executing the instruction comprises:

generating a result based on the at least one operand; and

storing the result at a second relative position in the local memory.

5. The method of Claim 4, wherein the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

6. A method of operating a cryptographic processor integrated circuit that comprises a local memory, the method comprising:

executing an instruction using the cryptographic processor that references at least one operand using a first relative position in the local memory.

7. The method of Claim 6, wherein executing the instruction comprises:

generating a result based on the at least one operand; and

storing the result at a second relative position in the local memory.

8. The method of Claim 7, wherein the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

9. A method of operating a cryptographic data processing system that comprises a host processor and a cryptographic processor integrated circuit coupled to the host processor, the method comprising:

providing a plurality of execution units in the cryptographic processor;

providing respective ones of a plurality of command blocks to respective ones of the plurality of execution units using the host processor; and

executing the plurality of command blocks using the plurality of execution units so that at least a portion of the execution of the plurality of command blocks is carried out simultaneously.

10. The method of Claim 9, wherein a system memory is coupled to the host processor and the cryptographic processor integrated circuit is coupled to the system memory, and wherein providing the respective ones of the plurality of command blocks to the respective ones of the plurality of execution units comprises:

providing a plurality of command queues in the system memory; and

loading the respective ones of the plurality of command blocks into respective ones of the plurality of command queues using the host processor.

11. The method of Claim 9, wherein the plurality of execution units comprise a random number generator unit, an encryption/authentication unit, and a public key engine unit.

12. A cryptographic data processing system, comprising:

a system memory; and

a cryptographic processor that is coupled to the system memory and comprises a plurality of execution units, each of the execution units comprising a command interface manager that load respective ones of a plurality of command blocks stored in the system memory to respective ones of the execution units for parallel execution thereon independent of whether another of the execution units is executing a command block.

13. The cryptographic data processing system of Claim 12, further comprising:

a host processor coupled to the system memory and being configured to load the system memory with the plurality of command blocks.

14. The cryptographic data processing system of Claim 13, wherein the system memory comprises a plurality of command queues that contain the plurality of command blocks, and wherein respective ones of the command interface managers are configured to independently load respective ones of the plurality of command blocks from respective ones of the plurality of command queues to respective ones of the execution units for parallel execution thereon.

15. The cryptographic data processing system of Claim 12, wherein the plurality of execution units comprise a random number generator unit, an encryption/authentication unit, and a public key engine unit.

16. A cryptographic data processing system that comprises a host processor, a system memory coupled to the host processor, and a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory, the system further comprising:

means for loading at least one operand from the system memory to the local memory; and

means for executing an instruction using the cryptographic processor that references the at least one operand using a first relative position in the local memory.

17. The cryptographic data processing system of Claim 16, wherein the means for loading at least one operand from the system memory to the local memory comprises means for loading at least two operands from the system memory to the local memory, and the means for executing the instruction comprises:

means for executing the instruction using the cryptographic processor that references a first one of the operands using the first relative position in the local memory and a second one of the operands using a second relative position in the local memory, the first and second relative positions being contiguous with one another.

18. The method of Claim 17, wherein the first one of the operands and the second one of the operands comprise different numbers of bits.

19. The cryptographic data processing system of Claim 16, wherein the means for executing the instruction comprises:

means for generating a result based on the at least one operand; and

means for storing the result at a second relative position in the local memory.

20. The cryptographic data processing system of Claim 19, wherein the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

21. A cryptographic processor integrated circuit that comprises:

a local memory; and

means for executing an instruction using the cryptographic processor that references at least one operand using a first relative position in the local memory.

22. The cryptographic processor integrated circuit of Claim 21, wherein the means for executing the instruction comprises:

means for generating a result based on the at least one operand; and

means for storing the result at a second relative position in the local memory.

23. The cryptographic processor integrated circuit of Claim 22, wherein the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

24. A cryptographic data processing system that comprises a host processor and a cryptographic processor integrated circuit coupled to the host processor, the system further comprising:

means for providing a plurality of execution units in the cryptographic processor;

means for providing respective ones of a plurality of command blocks to respective ones of the plurality of execution units using the host processor; and

means for executing the plurality of command blocks using the plurality of execution units so that at least a portion of the execution of the plurality of command blocks is carried out simultaneously.

25. The cryptographic data processing system of Claim 24, wherein a system memory is coupled to the host processor and the cryptographic processor integrated circuit is coupled to the system memory, and wherein the means for providing the respective ones of the plurality of command blocks to the respective ones of the plurality of execution units comprises:

means for providing a plurality of command queues in the system memory; and

means for loading the respective ones of the plurality of command blocks into respective ones of the plurality of command queues using the host processor.

26. The cryptographic data processing system of Claim 24, wherein the plurality of execution units comprise a random number generator unit, an encryption/authentication unit, and a public key engine unit.

27. A computer program product for operating cryptographic data processing system that comprises a host processor, a system memory coupled to the host processor, and a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory, the computer program product comprising:

a computer readable program medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code for loading at least one operand from the system memory to the local memory; and

computer readable program code for executing an instruction using the cryptographic processor that references the at least one operand using a first relative position in the local memory.

28. The computer program product of Claim 27, wherein the computer readable program code for loading at least one operand from the system memory to the local memory comprises computer readable program code for loading at least two operands from the system memory to the local memory, and the computer readable program code for executing the instruction comprises:

computer readable program code for executing the instruction using the cryptographic processor that references a first one of the operands using the first relative position in the local memory and a second one of the operands using a second relative position in the local memory, the first and second relative positions being contiguous with one another.

29. The computer program product of Claim 28, wherein the first one of the operands and the second one of the operands comprise different numbers of bits.

30. The computer program product of Claim 27, wherein the computer readable program code for executing the instruction comprises:

computer readable program code for generating a result based on the at least one operand; and

computer readable program code for storing the result at a second relative position in the local memory.

31. The computer program product of Claim 30, wherein the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

32. A computer program product for operating a cryptographic processor integrated circuit that comprises a local memory, the computer program product comprising:

a computer readable program medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code for executing an instruction using the cryptographic processor that references at least one operand using a first relative position in the local memory.

33. The computer program product of Claim 32, wherein the computer readable program code for executing the instruction comprises:

computer readable program code for generating a result based on the at least one operand; and

computer readable program code for storing the result at a second relative position in the local memory.

34. The computer program product of Claim 33, wherein the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

35. A computer program product for operating a cryptographic data processing system that comprises a host processor and a cryptographic processor integrated circuit coupled to the host processor, the computer program product comprising:

a computer readable program medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code for providing a plurality of execution units in the cryptographic processor;

computer readable program code for providing respective ones of a plurality of command blocks to respective ones of the plurality of execution units using the host processor; and

computer readable program code for executing the plurality of command blocks using the plurality of execution units so that at least a portion of the execution of the plurality of command blocks is carried out simultaneously.

36. The computer program product of Claim 35, wherein a system memory is coupled to the host processor and the cryptographic processor integrated circuit is coupled to the system memory, and wherein the computer readable program code for providing the respective ones of the plurality of command blocks to the respective ones of the plurality of execution units comprises:

computer readable program code for providing a plurality of command queues in the system memory; and

computer readable program code for loading the respective ones of the plurality of command blocks into respective ones of the plurality of command queues using the host processor.

37. The computer program product of Claim 35, wherein the plurality of execution units comprise a random number generator unit, an encryption/authentication unit, and a public key engine unit.

38. A method of operating a cryptographic processor, comprising:

dividing functions of the cryptographic processor into a plurality of execution units; and

providing commands to the execution units independent of whether another of the execution units is processing a command.

39. The method of Claim 38, wherein the execution units comprise at least one of an encryption/authentication execution unit, a public key engine execution unit, and a random number generator execution unit.

40. The method of Claim 38, wherein at least a portion of the execution of the commands is carried out simultaneously by the execution units.